UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/972,371	10/05/2001	Ryuichi Iwamura	SONY-50R4813	4728

7590 08/05/2009

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
08/05/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RYUICHI IWAMURA

Appeal 2008-004907
Application 09/972,371[1]
Technology Center 2400

Decided: August 5, 2009

Before JEAN R. HOMERE, ST. JOHN COURTENAY, III, and CAROLYN D. THOMAS, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1 through 7 and 17 through 20. Claims 8 through 16 and

[1] Filed on October 5, 2001. This application is a continuation-in-part to 09/696,584, filed on October 24, 2000. The real party in interest is Sony Electronics, Inc.

21 through 25 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Appellant's Invention

Appellant invented a method and system for decrypting and decoding a signal without exposing an encryption key on a communication bus. (Spec. 5, ll. 10-12.) Figure 4 depicts the steps of a process (400) for securely processing a digital signal. (Spec. 18, ll. 11-12.) In step 401, a public key is determined and exchanged between a conditional access block (230) and a central processing unit ("CPU") (160). (Spec. 18, ll. 19-21.) Further, both the conditional access block (230) and the CPU (16) internally generate their own private key. (Spec. 18, ll. 21-22.) In step 405, the conditional access block (239) receives an encrypted bit stream. (Spec. 19, ll. 4-5.) In step 410 and 420 respectively, the CPU (160) determines and encrypts the decryption key for the encrypted bit stream using the public key determined in step 401 and its own private key. (Spec. 19, ll. 7-14.) In step 430, the encrypted decryption key is transferred across a communication link via a bus to the conditional access block (230). (Spec. 19, ll. 20-22.) In step 440, the local processor located in the conditional access block (230) decrypts the encrypted decryption key utilizing the public key determined in step 401 accessed from local memory. (Spec. 19, l. 24 through Spec. 20, l. 3.) In step 450, the decrypted decryption key is used to decrypt the encrypted bit stream. (Spec. 20, ll. 5-6.)

Illustrative Claim

Independent claim 1 further illustrates the invention as follows:

1. A method of securely processing a digital signal comprising:

a) generating a public encryption key for use with a first logical circuit and a second logical circuit separate from said first logical circuit; in a digital media receiving device:

b) accessing an encrypted signal at said first logical circuit;

c) determining a first decryption key for said encrypted signal at said second logical circuit;

d) encrypting said first decryption key at said second logical circuit by use of said public encryption key;

e) transferring said encrypted first decryption key from said second logical circuit to said first logical circuit over a communication link;

f) at said first logical circuit, decrypting said encrypted first decryption key by use of a secret key to determine said first decryption key; and

g) at said first logical circuit, decrypting said encrypted signal using said first decryption key.

Prior Art Relied Upon

The Examiner relies on the following prior art as evidence of unpatentability:

Deo	US 5,721,781	Feb. 24, 1998
Spies	US 6,055,314	Apr. 25, 2000
Johnston	US 6,373,946 B1	Apr. 16, 2002 (filed Dec. 23, 1997)

Bruce Schneier, *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*, 513-14 (John Wiley & Sons, 1996) (hereinafter "Schneier").

John Watkinson, *The MPEG Handbook*, 366-81, 389-94 (Focal Press, 2nd ed. 2004) (hereinafter "Watkinson").

Rejections on Appeal

The Examiner rejects the claims on appeal as follows:

Claims 17 through 20 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Johnston.

Claims 1 and 3 through 7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Spies and Deo.

Claim 2 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Spies, Deo, and Schneier.

Appellant's Contentions

1. Appellant contends that the Examiner erred in finding that Johnston anticipates independent claim 17. In particular, Appellant argues that:

(a) While Johnson's disclosure teaches a digital mobile telecommunication system that includes mobile terminals, it does not teach a digital media receiving device, as recited in independent claim 17. (App. Br. 9-10.)

(b) Johnson's disclosure of encrypting data to be transmitted does not teach encrypting a digital signal in a receiving device. (App. Br. 10-11.)

(c) Johnson's disclosure of decrypting a received signal teaches away from encrypting a received signal. (App. Br. 11.)

2. Appellant contends that the Examiner erred in finding that Johnston anticipates dependent claim 19. In particular, Appellant argues that:

(a) Johnston's disclosure of a subscriber that has no access to data stored in the SIM teaches away from a modified local memory contained within the first logical circuit, the modifiable local memory enabling the modification of a computer control program stored within the local memory, as recited in dependent claim 19. (App. Br. 11-12.)

(b) Johnston's disclosure that all user terminals are provided with reprogrammable SIM cards does not teach modification of a computer control program, let alone that respective modifications take place within a digital media receiving device. (App. Br. 12.)

3. Appellant contends that the Examiner erred in concluding that the combination of Spies and Deo renders independent claim 1 unpatentable. In particular, Appellant argues that:

(a) Deo's disclosure of an authentication system that is dependent upon a hardware device comprising global secrets teaches away from Spies' disclosure of a system that has no global secrets. (App. Br. 14.)

(b) Deo's disclosure of entering a personal identification number ("PIN") into a terminal, in conjunction with a three-tiered authentication system, would render Spies inoperable for its intended purpose. (App. Br. 15-16.)

(c) Deo is nonanalogous art. (App. Br. 16-17.)

(d) Spies' disclosure of not permitting the view computing unit to read decryption capabilities and view individual packet data teaches away from at the first logical circuit, decrypting the encrypted signal using the first decryption key, as recited in independent claim 1. (App. 17-18).

(e) Spies' does not teach d) encrypting the first decryption key at the second logical circuit by use of the public encryption key; e) transferring the encrypted first decryption key from the second logical circuit to the first logical circuit over a communication link; and f) at the first logical circuit, decrypting the encrypted first decryption key by use of a secret key to determine the first decryption key, as recited in independent claim 1. (App. Br. 19.)

4. Appellant contends that the Examiner erred in concluding that the combination of Spies and Deo renders dependent claim 4 unpatentable. In particular, Appellant argues that Spies' disclosure of changing and updating cryptographic service does not teach replacing a computer control program stored in a second portion of local memory at the second logical circuit with a new computer control program, as recited in dependent claim 4. (App. Br. 20-21.)

5. Appellant contends that the Examiner erred in concluding that the combination of Spies and Deo renders dependent claim 6 unpatentable.

In particular, Appellant argues that the Examiner's admission in the rejection entered February 17, 2006, concedes that the combination of Spies and Deo does not teach a decryption routine that can be updated and replaced. (App. Br. 21.)

6. Appellant contends that the Examiner erred in concluding that the combination of Spies and Deo renders dependent claim 7 unpatentable. In particular, Appellant argues that:

(a) Spies' disclosure of video content that includes TV cable, satellite networks, and digital video disks ("DVDs") does not teach wherein the digital signal is substantially compliant with the Motion Pictures Experts Group ("MPEG") format, as recited in dependent claim 7. (App. Br. 22-24.)

(b) The Examiner's reliance on Watkinson as rebuttal evidence is improper because it does not qualify as prior art. (App. Br. 22-23.)

(c) The Examiner cannot rely on inherency because Spies discloses video content that includes game CDs and on-line networks that may use non-MPEG encoding. (App. Br. 24.)

7. Appellant contends that the Examiner erred in concluding that the combination of Spies, Deo, and Schneier renders dependent claim 2 unpatentable. In particular, Appellant argues that:

(a) Spies' disclosure of not permitting the view computing unit to read decryption capabilities and view individual packet data teaches away from generating the public encryption key using the technique of Diffie-Hellman Key Exchange, as recited in dependent claim 2. (App. Br. 26-27.)

(b) Deo's disclosure of certifying an authority by transferring keys via certifications teaches away from generating the public encryption key using the technique of Diffie-Hellman Key Exchange, as recited in dependent claim 2. (App. Br. 27.)

Examiner's Findings and Conclusions

1. The Examiner finds that Johnston anticipates independent claim 17. In particular, the Examiner avers that:

(a) Johnston's disclosure of a voice communications system in a digital format, including a mobile phone, teaches a digital media receiving device, as recited in independent claim 1. (Ans. 8.)

(b) Independent claim 17 does not explicitly require encrypting data on reception. (Ans. 8.) Further, Johnston's disclosure of receiving an encryption key from a SIM card and encrypting a digital signal within a mobile phone teaches a second logical circuit for encrypting the digital signal using the local encrypting key accessed from the first logical circuit, as recited in independent claim 17. (Ans. 8-9.)

(c) Independent claim 17 does not explicitly require encrypting a received signal. (Ans. 9.)

2. The Examiner finds that Johnston anticipates dependent claim 19. In particular, the Examiner avers that:

(a) Dependent claim 19 requires only that the memory could be modified, not that it actually is modified. (Ans. 9.) Further, Johnston's disclosure of reprogramming SIM cards used in mobile phones teaches a modified local memory contained within the first logical circuit, the modifiable local memory enabling the modification of a computer control program stored within the local memory, as recited in dependent claim 19. (Ans. 9-10.)

(b) Dependent claim 19 does not require the memory to be modified within a digital media receiving device. (Ans. 9-10.)

3. The Examiner concludes that the combination of Spies and Deo renders independent claim 1 unpatentable. In particular, the Examiner finds that:

(a) Deo's disclosure of digital certificates as public key certificates, in conjunction with Spies' disclosure of a public and private key pair, teaches securely processing a digital signal by encrypting a key utilizing a public key encryption technique before transferring it across a communication link, as recited in independent claim 1. (Ans. 10-11.)

(b) The combined teachings of Spies and Deo would have suggested to an ordinarily skilled artisan encrypting the decryption key with the public key of the set top box prior to transmitting the decryption key to the set top box. (Ans. 11.)

(c) Deo is analogous art because it provides design incentives and other market forces to prompt variation of Spies. (Ans. 11-12.)

(d) Spies' disclosure of decrypting the encrypted video signal utilizing a key transmitted from the IC card to the processor, in conjunction with Deo's disclosure of secured communications between a smart card and a terminal, teaches at the first logical circuit, decrypting the encrypted signal using the first decryption key, as recited in independent claim 1. (Ans. 12.)

(e) Deo's disclosure of a smart card that encrypts data using a terminal's public key so that only the terminal can decrypt the data using its own private key teaches: d) encrypting the first decryption key at the second logical circuit by use of the public encryption key; e) transferring the encrypted first decryption key from the second logical circuit to the first logical circuit over a communication link; and f) at the first logical circuit, decrypting the encrypted first decryption key by use of a secret key to determine the first decryption key, as recited in independent claim 1. (An. 12-13.)

4. The Examiner concludes that the combination of Spies and Deo renders dependent claim 4 unpatentable. In particular, the Examiner finds that Spies' disclosure of changing or updating cryptographic service providers teaches replacing a computer control program stored in a second portion of local memory at the second logical circuit with a new computer control program, as recited in dependent claim 4. (Ans. 13-14.)

5. The Examiner concludes that the combination of Spies and Deo renders dependent claim 6 unpatentable. In particular, the Examiner finds that Spies' disclosure of changing or updating cryptographic service providers teaches replacing a computer control program stored in a second portion of local memory at the first logical circuit with a new computer control program, as recited in dependent claim 6. (Ans. 14.)

6. The Examiner concludes that the combination of Spies and Deo renders dependent claim 7 unpatentable. In particular, the Examiner finds that:

(a) Spies' disclosure of delivering video content to a set top box via satellite TV networks inherently teaches MPEG format. (Ans. 14, 16.)

(b) Watkinson was introduced as rebuttal evidence to support the Examiner's position that MPEG format was inherent in video distribution over satellite TV. (Ans. 15.)

7. The Examiner concludes that the combination of Spies, Deo, and Schneier renders dependent claim 2 unpatentable. In particular, the Examiner finds that Schneier's disclosure of utilizing the Diffie-Hellman algorithm for public key exchange teaches generating the public key encryption using the technique of Diffie-Hellman Key Exchange. (Ans.17-18.)

II. ISSUES

1. Has Appellant shown that the Examiner erred in finding that Johnston anticipates independent claim 17? In particular, the issue turns on whether Johnston teaches a digital media receiving device and a second logical circuit for encrypting the digital signal, as recited in independent claim 17.

2. Has Appellant shown that the Examiner erred in finding that Johnston anticipates dependent claim 19? In particular, the issue turns on whether Johnston teaches a modified local memory contained within the first logical circuit, the modifiable local memory enabling the modification of a computer control program stored within the local memory, as recited in dependent claim 19.

3. Has Appellant shown that the Examiner erred in concluding that the combination of Spies and Deo renders independent claim 1 unpatentable? In particular, the issue turns on whether:

(a) Deo and Spies may be properly combined.

(b) The proffered combination teaches: d) encrypting the first decryption key at the second logical circuit by use of the public encryption key; e) transferring the encrypted first decryption key from the second logical circuit to the first logical circuit over a communication link; f) at the first logical circuit, decrypting the encrypted first decryption key by use of a secret key to determine the first decryption key; and g) at the first logical circuit, decrypting the encrypted signal using the first decryption key, as recited in independent claim 1.

4. Has Appellant shown that the Examiner erred in concluding that the combination of Spies and Deo renders dependent claim 4 unpatentable? In particular, the issue turns on whether Spies teaches replacing a computer control program stored in a second portion of local memory at the second logical circuit with a new computer control program, as recited in dependent claim 4.

5. Has Appellant shown that the Examiner erred in concluding that the combination of Spies and Deo renders dependent claim 6 unpatentable? In particular, the issue turns on whether Appellant can rely on the Examiner's admission in the Final Rejection entered February 17, 2006.

6. Has Appellant shown that the Examiner erred in concluding that the combination of Spies and Deo renders dependent claim 7 unpatentable? In particular, the issue turns on whether:

(a) Spies teaches that the digital signal is substantially compliant with the MPEG format, as recited in dependent claim 7.

(b) The Examiner can rely on Watkinson as rebuttal evidence to support the Examiner's position that MPEG format was inherent in Spies' disclosure of video distribution over TV cable or satellite networks.

7. Has Appellant shown that the Examiner erred in concluding that the combination of Spies, Deo, and Schneier renders dependent claim 2 unpatentable? In particular, the issue turns on whether Schneier teaches generating the public encryption key using the technique of Diffie-Hellman Key Exchange, as recited in dependent claim 2.

III. FINDINGS OF FACT

The following Findings of Fact ("FF") are shown by a preponderance of the evidence.

Appellant's Invention

1. In order to combat theft of encryption keys on a communication link, embodiments of the present invention encrypt the key itself by means of a public key encryption technique before transferring it across a communication link. (Spec. 11, ll. 16-19.)

2. One well-known method of determining a public key is the Diffie-Hellman Key Exchange technique. (Spec. 12, ll. 5-7; Spec. 13, ll. 9-10; Spec. 18, ll. 22-23.)

Johnston

3. Johnston discloses a method and apparatus for providing secure communication through a communications network. (Col. 1, ll. 7-9.) Further, Johnston discloses that digital mobile voice communications systems are well known. (Col. 1, ll. 13-14.)

4. Figure 2 depicts mobile terminal equipment in the form of a handset comprising a digital coder/decoder (30), a control circuit (37) consisting of a microprocessor, and a SIM card (35) that includes a processor (35a) and permanent memory (35b). (Col. 5, ll. 50-60; Col. 6, ll. 9-12, 20-23.)

5. Figure 13 depicts that the SIM receives the partial key and in step 1304 the SIM reads the terminal key from within the memory (35b). (Col. 10, ll. 36-38.) In step 1306, the SIM processor (35a) recovers the binary number RAND by comparing the stored terminal key K_a from the partial key K_{pa}, to generate a new 128 bit binary number. (Col. 10, ll. 38-41.) Thus, the SIM processor computes a code K_R. (Col 10, ll. 42-43.) The SIM card (35) supplies K_R=(RAND) the card reader device (33) to the terminal processor (37). (Col. 10, ll. 51-52.) The code K_R is used as an enciphering key for data to be transmitted. (Col. 10, ll. 52-53.)

6. As depicted in Figure 17b, at each terminal, the SIM processor (35a) performs an additional step 1305 between steps 1304 and 1306. (Col. 12, ll. 20-22.) In step 1305, the received partial key is decrypted using the terminal key, prior to calculating the ciphering key. (Col. 12, ll. 22-24.)

7. All user terminals are provided with reprogrammed SIM cards that allow secure communication within the temporary group. (Col. 16, ll. 47-49.)

Spies

8. Spies discloses a system and method for secure purchase and delivery of video content programs over various distribution media, including distribution networks and digital video disks, that includes an

integrated circuit card (e.g. a smart card, PCM-CIA card) which is configured to store decryption capabilities for related video programs. (Abstract; Col. 1, ll. 7-11.)

9. Video content programs are commonly supplied to viewers in many different forms including TV cable and broadcasts systems. (Col. 1, ll. 14-17.) Valuable video content programs are distributed to consumers for home viewing over TV cable or satellite networks. (Col. 1, ll. 17-22.) With recent technology improvements, video content programs can also be delivered on DVDs. (Col. 1, ll. 22-24.)

10. Figure 6 depicts IC card (50) implemented as a smart card. (Col. 11, l. 26.) IC card (50) has a CPU (100), a volatile rewriteable Random Access Memory ("RAM") (102), a Read Only Memory ("ROM") (104), and Electrically Erasable Programmable ROM ("EEPROM") (106). (Col. 11, ll. 26-30.) The cryptographic service providers ("CSPs") (118 and 120) are preferably implemented in software in dynamic linked libraries ("DLLs") which are stored in the ROM (104). (Col. 11. 64-66.) This implementation is advantageous because it is easily invoked and dynamically accessible by an application running on the CPU (100). (Col. 11, l. 66 through Col. 12, l. 1.) Furthermore, the cryptographic functions can be changed or updated simply by replacing one or more DLLs. (Col. 12, ll. 1-3.)

11. Figure 7 depicts the viewer computing unit (60) and its interface with the IC card (50). (Col. 12, 39-40.) The video input (158) receives the digital video data in its encrypted form. (Col. 12, ll. 61-62.) The video input can be configured to remove the packet key from the security header and pass it through the card I/O (160) to IC card (50). (Col.

12, ll. 62-64.) The IC card (50) executes a view CSP (120) to expand the packet key K_i to the expanded key $E_x(K_i)$ using the program key (118) stored in its EEPROM (116). (Col. 12, l. 66 through Col. 13, l. 2.) The expanded key $E_x(K_i)$ is outputted from the IC card (50) and transferred to the processor (150). (Col. 13, ll. 2-3.) A decryption routine (162) stored in program memory (152) is executed on the processor (150) to produce the random set of bits from the expanded key $E_x(K_i)$, and to combine the random set of bits with the encrypted data payload to reproduce the original digital video data. (Col. 13, ll. 3-8.)

Deo

12. Deo discloses a smart card authentication system that verifies the user, smart card, application, and terminal. (Col. 2, ll. 55-57.)

13. To establish communication, the smart card uses the terminal's public key that it received in the terminal's certificate to send a message. (Col. 7, ll. 1-3.) Only the terminal can decrypt the message using its private key. (Col. 7, ll. 3-4.) Similarly, the terminal can encrypt a reply message using the smart card's public key and only the smart card can decrypt the message. (Col. 7, ll. 4-6.)

Schneier

14. Schneier discloses that Diffie-Hellman was the first public-key algorithm every invented, way back in 1976. (Pg. 513, l. 1.)

Watkinson

15. Watkinson discloses that digital television broadcasting relies on the combination of a number of fundamental technologies, including MPEG. (Pg. 368, ll. 21-24.) Digital video broadcasting ("DVB") is a

standard that incorporates MPEG-2 picture and sound coding. (Pg. 369, ll. 7-10.)

IV. PRINCIPLE OF LAW

Anticipation

In rejecting claims under 35 U.S.C. § 102, "[a] single prior art reference that discloses, either expressly or inherently, each limitation of a claim invalidates that claim by anticipation." *Perricone v. Medicis Pharmaceutical Corp.*, 432 F.3d 1368, 1375 (Fed. Cir. 2005) (citing *Minn. Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.*, 976 F.2d 1559, 1565 (Fed. Cir. 1992)). "Anticipation of a patent claim requires a finding that the claim at issue 'reads on' a prior art reference." *Atlas Powder Co. v. IRECO, Inc.*, 190 F.3d 1342, 1346 (Fed Cir. 1999). "In other words, if granting patent protection on the disputed claim would allow the patentee to exclude the public from practicing the prior art, then that claim is anticipated, regardless of whether it also covers subject matter not in the prior art." *Id.* (internal citations omitted).

Obviousness

"On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness." *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998).

> Section 103 forbids issuance of a patent when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at

> the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains."

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 406 (2007).

In *KSR*, the Supreme Court emphasized "the need for caution in granting a patent based on the combination of elements found in the prior art," and discussed circumstances in which a patent might be determined to be obvious. *Id.* at 415 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 12 (1966)). The Court reaffirmed principles based on its precedent that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* at 416. The operative question in this "functional approach" is thus "whether the improvement is more than the predictable use of prior art elements according to their established functions." *Id.* at 417.

In identifying a reason that would have prompted a person of ordinary skill in the relevant field to combine the prior art teachings, the Examiner must show some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *Id.* at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

Inherency

"In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic *necessarily* flows from the teachings of the applied prior art." *Ex parte Levy*, 17 USPQ2d

1461, 1464 (BPAI 1990). "[A]fter the PTO establishes a prima facie case of anticipation based on inherency, the burden shifts to appellant to 'prove that the subject matter shown to be in the prior art does not possess the characteristic relied on.'" *In re King*, 801 F.2d 1324, 1327 (Fed. Cir. 1986) (quoting *In re Swinehart*, 439 F.2d 210, 212-13, (CCPA 1971)). There is no requirement that a person of ordinary skill in the art would have recognized the inherent disclosure at the time of invention, but only that the subject matter is in fact inherent in the prior art reference. *Schering Corp. v. Geneva Pharm. Inc.*, 339 F.3d 1373, 1377 (Fed. Cir. 2003).

Teaching Away

"What the prior art teaches and whether it teaches toward or away from the claimed invention . . . is a determination of fact." *Para-Ordnance Mfg., Inc. v. SGS Importers Int'l, Inc.*, 73 F.3d 1085, 1088 (Fed. Cir. 1995). "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994). Teaching an alternative or equivalent method, however, does not teach away from the use of a claimed method. *In re Dunn*, 349 F.2d 433, 438 (CCPA 1965).

V. CLAIM GROUPING

Appellant argues that Johnston does not anticipate independent claim 17 and that the combination of Spies and Deo does not render independent claim 1 unpatentable. Further, Appellant separately argues claims 2, 4, 6, 7, and 19. In accordance with the provisions of 37 C.F.R. § 41.37 (c)(1)(viii), we will consider claims 18 and 20 as standing or falling with claim 17. Claims 3 and 5 stand or fall with claim 1.

VI. ANALYSIS

35 U.S.C. § 102-Johnston

Claim 17

Independent claim 17 recites, in relevant parts: 1) in a digital media receiving device; and 2) a second logical circuit for encrypting the digital signal using a local encryption key accessed from a first logical circuit.

As set forth in the Findings of Fact section, Johnston discloses providing secure communication through a communications network. (FF 3.) In particular, Johnston discloses that digital mobile voice communications systems are well known. (*Id.*) Further, Johnston discloses a mobile terminal comprising a digital coder/decoder (30), a control circuit (37) consisting of a microprocessor, and a SIM card (35) that includes a processor (35a) and a permanent memory (35b). (FF 4.) We find that Johnston's disclosure teaches a mobile terminal that provides digital voice communications. Further, we find that, by providing digital voice communications, the disclosed mobile terminal teaches a digital media receiving device.

Further, Johnston discloses that the SIM receives a partial key and reads the terminal key from within its memory (35b). (FF 5.) At each terminal, the received partial key is decrypted using the terminal key prior to calculating the ciphering key. (FF 7.) The SIM processor (35a) recovers the binary number RAND by comparing the stored terminal key K_a from the partial key K_{pa}, to generate a new binary number and compute a code K_R. (FF 5.) The SIM card (35) supplies an enciphering key to the terminal processor (37) for data to be transmitted. (*Id.*) We find that Johnston's disclosure teaches that the SIM card utilizes a partial key to calculate an encryption key and, further, provides the encryption key to the processor contained in the mobile terminal for encrypting data transmissions. In particular, we find that Johnston's disclosure of a SIM card that provides the encryption key to the processor contained in the mobile terminal for encrypting data transmissions teaches a second logical circuit for encrypting the digital signal using a local encryption key accessed from a first logical circuit, as recited in independent claim 17.

Claim 19

Dependent claim 19 recites, in relevant part, a modifiable local memory contained within the first logical circuit, the modifiable local memory enabling the modification of a computer control program stored within the local memory.

As discussed above, Johnston discloses a SIM card (35) that includes a processor (35a) and a permanent memory (35b). (FF 4.) Further, Johnston discloses that all user terminals are provided with reprogrammed SIM cards that allow secure communication. (FF 7.) We find that Johnston's disclosure teaches a SIM card with a memory that can be reprogrammed or modified accordingly. In particular, we find that Johnston's disclosure of a

SIM card with a memory that can be reprogrammed or modified accordingly teaches a modifiable local memory contained within the first logical circuit, the modifiable local memory enabling the modification of a computer control program stored within the local memory, as recited in dependent claim 19.

Teaching Away

Appellant further argues that the Johnston reference "teaches away" from independent claim 17 and dependent claim 19. (App. Br. 11, 12.) We find that Appellant's "teaching away" argument is misplaced because the Examiner has rejected the claims under 35 U.S.C. § 102. Our reviewing court has determined that "[t]eaching away is irrelevant to anticipation." *Seachange International, Inc., v. C-Cor, Inc.*, 413 F.3d 1361, 1380 (Fed. Cir. 2005).

35 U.S.C. § 103-Spies and Deo

Claim 1

Independent claim 1 recites, in relevant parts:

> d) encrypting [the] first decryption key at [the] second logical circuit by use of [the] public encryption key; e) transferring [the] encrypted first decryption key from [the] second logical circuit to [the] first logical circuit over a communication link; f) at [the] first logical circuit, decrypting [the] encrypted first decryption key by use of a secret key to determine [the] first decryption key; and g) at [the] first logical circuit, decrypting [the] encrypted signal using [the] first decryption key.

As set forth in the Findings of Fact section, Spies discloses a system and method for secure purchase and delivery of video content programs that includes a smart card configured to store decryption capabilities for related video programs. (FF 8.) Deo discloses a smart card authentication system that verifies the user, smart card, application, and terminal. (FF 12.) In particular, the smart card uses a public key that it received in the terminal's certificate to send a message. (FF 13.) Only the terminal can decrypt the message using its private key. (*Id.*) We find that Spies and Deo disclose prior art elements that perform their ordinary functions to predictably result in a method of securely processing a digital signal by encrypting a key utilizing a public key encryption technique before transferring it across a communication link. *See KSR*, 550 U.S. at 416-17.

We are not persuaded by Appellant's argument that Deo's disclosure of an authentication system that is dependent upon hardware comprising global secrets teaches away from Spies' disclosure of a system that has no global secrets. (App. Br. 14.) As set forth above, Deo discloses that the smart card uses a public key that is received in the terminal's certificate to send a message. (FF 13.) Only the terminal can decrypt the message using its private key. (*Id.*) We find that Deo's disclosure teaches digital certificates that are public key certificates. In particular, we agree with the Examiner that public key certificates are not to be confused with global secrets because the public key certificates are "published" by definition, whereas global secrets are not. (Ans. 10.) Further, we are not persuaded by Appellant's argument that Deo's disclosure of entering a PIN into a terminal, in conjunction with a three-tiered authentication system, would render Spies inoperable for its intended purpose. (App. Br. 15-16.) As set forth above, Deo discloses a smart card authentication system that verifies the user, smart card, application, and terminal. (FF 12.) We find that Deo discloses an authentication system that verifies a smart card and respective terminal. In particular, we find that an ordinarily skilled artisan would recognize that entering a PIN into a terminal and utilizing a three-tiered authentication system simply promotes security by reinforcing the authentication of users. Thus, we conclude that Deo's disclosure of entering a PIN into a terminal and utilizing a three-tiered authentication system does not undesirably encumber the purpose of authentication nor does it inherently change Spies' disclosure of securely purchasing and delivering video content programs.

Upon reviewing Appellant's Specification, Appellant indicates that the claimed invention generally relates to combating theft of encryption keys on a communication link, whereby the key itself is encrypted by means of a public key encryption technique before transferring it across a communication link. (FF 1.) We find that Appellant's field of endeavor is encryption of data. As set forth above, Deo discloses a smart card authentication system that verifies the user, smart card, application, and terminal. (FF 12.) In particular, the smart card uses a public key that it received in the terminal's certificate to send a message. (FF 13.) Only the terminal can decrypt the message using its private key. (*Id.*) We find that Deo is within the same field of endeavor as the claimed invention because both concern encryption of data.

As set forth in the Findings of Fact section, Spies discloses a viewer computing unit (60) and a respective IC card (50). (FF 11.) After the viewer computing unit (60) receives encrypted digital video data, the IC card (50) transmits the encrypted digital video data and an expanded encryption key to the processor. (*Id.*) The viewer program memory (152) of the processor utilizes a decryption routine to decrypt and reproduce the original digital video data. (*Id.*) We find that Spies' disclosure teaches a viewing computing unit containing a processor that utilizes a decryption key to decrypt the encrypted digital video data. In particular, we find that Spies' disclosure of a viewing computing unit that contains a processor that utilizes a decryption key to decrypt the encrypted digital video data teaches at the first logical circuit, decrypting the encrypted signal using the first decryption key, as recited in independent claim 1. We are not persuaded by Appellant's argument that the viewing computing unit (60) in Spies is incapable of decryption. (App. Br. 18.)

Further, Appellant argues that Spies teaches away from the claim invention. (App. Br. 17-18.) We do not agree. As set forth above, we find that Spies teaches a viewing computing unit that contains a processor that utilizes a decryption key to decrypt the encrypted digital video data. Appellant has shown nothing in Spies that would have discouraged a person of ordinary skill in the art from decrypting encrypted digital video data within a viewing computing unit that contains a processor. Appellant has not pointed to an explicit disclosure within Spies stating that the viewing computing unit that contains a processor cannot decrypt the encrypted digital video data. Instead, we view Spies' disclosure of a viewing computing unit that utilizes a decryption key to decrypt the encrypted digital video data as an alternative or equivalent teaching to at the first logical circuit, decrypting the encrypted signal using the first decryption key. Therefore, Appellant has not shown that Spies' disclosure of a viewing computing unit that utilizes a decryption key to decrypt the encrypted digital video data teaches away from the claimed at the first logical circuit, decrypting the encrypted signal using the first decryption key, as recited in independent claim 1.

For subsections (d), (e), and (f) of claim 1, Appellant reproduces the language of the claim verbatim and asserts that Spies fails to teach the respective limitations. However, Appellant makes no attempt to compare and contrast the claimed invention with the cited textual portions relied upon by the Examiner to establish the alleged distinction. Appellant is reminded that a statement that merely points out what the claim recites will not be considered as an argument for separate patentability of a claim. 37 C.F.R. § 41.37(c)(1)(vii). Appellant is further reminded that a general allegation that the claim defines a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references does not constitute a persuasive response. 37 C.F.R. § 1.111(b). Therefore, Appellant's arguments are unpersuasive. It follows that Appellant has not shown that the Examiner erred in concluding that the combination of Spies and Deo renders independent claim 1 unpatentable.

Claim 4

Dependent claim 4 recites, in relevant part, replacing a computer control program stored in a second portion of local memory at the second logical circuit with a new computer control program.

As set forth in the Findings of Fact section, Spies discloses an IC card (50) that has a CPU (100) and a ROM (104). (FF 10.) The CSPs (118 and 120) are preferably implemented in the software stored in the ROM (104) and can be changed or updated. (*Id.*) We find that Spies' disclosure teaches an IC card that includes a ROM that contains cryptographic functions that can be changed or updated. In particular, we find that Spies' disclosure of an IC card that includes a ROM containing cryptographic functions that can be changed or updated teaches replacing a computer control program stored in a second portion of local memory at the second logical circuit with a new computer control program, as recited in dependent claim 4. We are not persuaded by Appellant's arguments that changing software stored in a ROM requires the physical replacement of the ROM device or that the ROM cannot be replaced. (App. Br. 20-21.) It follows that Appellant has not shown that the Examiner erred in concluding that the combination of Spies and Deo renders dependent claim 4 unpatentable.

Claim 6

We are not persuaded by Appellant's argument that the Final Rejection entered February 17, 2006, admits that Spies and Deo does not disclose that the decryption routine can be update or replaced. (App. Br. 21.) The Final Rejection entered February 17, 2006, is not under appeal. It follows that Appellant has not shown that the Examiner erred in concluding that the combination of Spies and Deo renders dependent claim 6 unpatentable.

Claim 7

Dependent claim 7 recites, in relevant part, wherein the digital signal is substantially compliant with the MPEG format.

As set forth in the Findings of Fact, Spies discloses that video content programs are commonly supplied to viewers in many different forms and are distributed to consumers for home viewing over TV cable or satellite networks. (FF 9.) Additionally, Spies discloses that video content programs can also be delivered on DVDs. (*Id.*) We find that Spies' disclosure teaches distributing video content programs via TV cable, satellite networks, and DVDs. Further, Watkinson discloses that digital television broadcasting relies on the combination of a number of fundamental technologies, including MPEG. (FF 15.) DVB is a standard that incorporates MPEG-2 picture and sound coding. (*Id.*) We find that Watkinson's disclosure teaches that digital television and video broadcasting relies on MPEG format. In particular, we find that an ordinarily skilled artisan would recognize that digital signals substantially compliant with the MPEG format necessarily flows from Spies' teaching of distributing video content programs via TV cable, satellite networks, and DVDs.

We are not persuaded by Appellant's argument that Watkinson cannot be relied upon as rebuttal evidence to prove inherency. (App. Br. 22-23.) We agree that the Examiner has properly shifted the burden to Appellant by providing a rationale in the Answer that reasonably supports the Examiner's finding of inherency with respect to the Spies reference. Further, Appellant's allegation that Watkinson cannot be relied on as rebuttal evidence because the publication date is after the priority date of the claimed invention is unavailing. (App. Br. 22.) While an ordinarily skilled artisan may not have recognized Spies' inherent disclosure of MPEG format at the time of invention, it only suffices that the cited teaching is in fact inherent. *See Schering Corp.*, 339 F.3d at 1377; *see also* MPEP §§ 2124 and 2131.01. Since Appellant has failed to proffer any evidence to dispel the Examiner's position, we find that Appellant has not shown that the Examiner erred in concluding that the combination of Spies and Deo renders dependent claim 7 unpatentable.

35 U.S.C. § 103-Spies, Deo, and Schneier
Claim 2

Dependent claim 2 recites, in relevant part, generating the public encryption key using the technique of Diffie-Hellman Key Exchange.

As set forth in the Findings of Fact section, Schneier discloses that Diffie-Hellman was the first public-key algorithm invented in 1976. (FF 14.) We find that Schneier disclosure teaches generating a public key utilizing the Diffie-Hellman technique. Additionally, upon reviewing Appellant's Specification, Appellant admits that the Diffie-Hellman Key Exchange technique is a well-known method for determining a public key. (FF 2.) We find that the Diffie-Hellman Key Exchange is an old and well-known method for determining a public key. In summary, we find that

Schneier's disclosure of generating a public key utilizing the Diffie-Hellman technique, in conjunction with Appellant's admission, teaches generating said public encryption key using the technique of Diffie-Hellman Key Exchange, as recited in dependent claim 2. We are not persuaded by Appellant's argument that both Spies and Deo teach away from generating said public encryption key using the technique of Diffie-Hellman Key Exchange. (App. Br. 26-28.) It follows that Appellant has not shown that the Examiner erred in concluding that the combination of Spies, Deo, and Schneier renders dependent claim 2 unpatentable.

VII. CONCLUSIONS OF LAW

1. Appellant has not shown that the Examiner erred in finding that Johnston anticipates claims 17 through 20 under 35 U.S.C. § 102(e).

2. Appellant has not shown that the Examiner erred in concluding that the combination of Spies and Deo renders claims 1 and 3 through 7 unpatentable under 35 U.S.C. § 103(a).

3. Appellant has not shown that the Examiner erred in concluding that the combination of Spies, Deo, and Schneier renders claim 2 unpatentable under 35 U.S.C. § 103(a).

VIII. DECISION

We affirm the Examiner's decision to reject claim 17 through 20 as being anticipated under 35 U.S.C. § 102(e). We affirm the Examiner's decision to reject claims 1 through 7 as being unpatentable under 35 U.S.C. § 103(a).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

msc

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose CA 95113